الفيروسات وكيف تصمم

في مهاجمة الملفات

اعــــداد

عصام سرحان ذياب

Issam_art4@yahoo.com

الفهرست

- فيروسات الملفات
- الفيروسات التي تتصل بالملف المضيف Appending Viruses
- إصابة الملفات
- الفيروسات وأنظمة Windows
- فيروسات النظام Windowsعلى منصات عمل Windows
- أمثلة عن فيروسات نظام Windows

- الفصل الرابع :

- الفيروسات والانترنت واهم أنواع الفيروسات
- الفيروسات والانترنت
- لغة HTML
- بعض التقانات
- فيروسات البريد الالكتروني .
- برامج البريد الالكتروني
- أنماط البريد الالكتروني
- ديدان البريد الالكتروني
- أهم الفيروسات

الفصل الأول

الإطار النظري

المقدمة :

تعتبر الفيروسات المشكلة التي تواجه العصر المتطور أي القرن العشرين ولكن لم يطلق عليها اسم في ذلك الوقت وأول من سماها بهذا الاسم عام ١٩٨٣ هو Fred Cohen لكن في هذه السنين كانت ما تزال الفيروسات كائنا نظريا أي لم يكن الحديث عنها شائعا بين الناس ، ثم ما لبثت أن تطورت وأصبحت في أجهزة الحواسيب وقد أصبحت الحاجة ملحة إلى اكتشاف الفيروس المضاد .

في الماضي كانت وسيلة انتقال الفيروسات من حاسب لأخر عن طريق تبادل الاسطوانات المرنة فالفيروس الذي يصيب الحاسب يضع نفسه في الذاكرة الالكترونية ، وإذا أحس الفيروس إن الحاسوب يقوم بنقل ملف إلى وحدة الاسطوانات المرنة ، فانه يقوم بنقل ملف إلى وحدة الاسطوانات المرنة ، فانه يقوم بالالتصاق بهذا الملف حتى يتيح لنفسه فرصة إصابة حاسبة جديدة إذا ما قام هذا الحاسب بتشغيل الاسطوانة المصابة .

وبعدها جاء الانترنت ليقدم لمستخدميه خدمة البريد الالكتروني فوجدت الفيروسات وسيلة أكثر كفاءة للانتشار وإصابة اكبر عدد من الحاسبات ، ففيروسات البريد الالكتروني والتي يطلق عليها نوع الدودة تصل إلى حاسباتنا في صورة ملف ملحق بالرسالة الالكترونية ، فإذا أقمنا بتشغيل هذا الملف أو محاولة فتحه ينشط الفيروس لكي يصيب الحاسب .

فالفيروس هي نوع من البرامج التي يتم تطويرها لكي تحدث اثأرا تخريبية على الحاسبات التي تصيبها وهذه الفيروسات تكتب بإحدى لغات البرمجة التقليدية التي يستخدمها مطورو البرامج مثل لغة الفيجول بيسك او جافا يجب أن يكون الفيروس قادرا على الانتقال من حاسب إلى آخر لكي يضمن له طريقة جيدة للانتشار بين اكبر عدد من الحاسبات .

ظهر أول فيروس للحاسبات في أواخر الستينات فكان محددا نظرا لقلة عدد الحاسبات مما هو عليه ألان كما إن الحاسبات الشخصية لم تكن قد اخترعت وأيضا لم تكن هناك شبكات للانترنت .

الوضع تغير ألان وأصبح عدد الحاسبات الشخصية في العالم يقدر بمئات الملايين كما إن شبكة الانترنت يتصل بها ألان أكثر من مليار شخص أتاح للفيروسات قدرة كبيرة على الانتشار مستغلين شبكة الانترنت كوسيلة سريعة تحقق لمطورو الفيروسات أهدافهم الشريرة .

ويمكن القول إن الفيروس هو برنامج دخيل تخريبي يتم زرعه عادة ضمن أنظمة تشغيل الحواسيب أو الملفات الاعتيادية الشائعة الاستخدام بصورة مباشرة عن طريق وسائط الإدخال كالأقراص المرنة أو بصورة غير مباشرة من خلال الانتقال بين حواسيب الشبكة .

هدف البحث :

يهدف البحث إلى التعرف على اثر استخدام الفيروس على مستوى أجهزة الحاسوب وكيفية تصميمها في مهاجمة الملفات وبالتالي تكوين تعليمية ومفهومة على مستوى العامة لمعرفة وتعريف الفيروسات .

فرضية البحث :

تتحدد فرضية البحث من خلال بيان رؤية أساسية مفادها إن الفيروسات الهجومية تعمل على تخريب الحاسوب الذي تقوم بالسيطرة عليه وهي تنتشر بدون تمييز بين الحاسوب الذي لا يتسبب بضرر للحاسبة المصدرة للفيروس والحاسبة التي تسبب الضرر له وهي تستخدم شبكة الانترنت للانتشار والانتقال بينما تعمل الفيروسات الدفاعية على حماية نظم التشغيل الخاصة بالحاسبات نظم إدارة الملفات الخاصة بها من التدخل والتطفل من قبل أشخاص آخرين غير مخولين ، هدفهم السيطرة على تلك البرمجيات وسرقة المعلومات وهي ذات انتشار محدد ولا تنشط إلا في حال التعدي على الجهاز المصدر لها أو سرقة إحدى منتجاتها البرمجية الغير مرخصة للشخص الذي يقوم بسرقة تلك البيانات ، وبالتالي فالفيروسات هي حقيقة علمية على مستوى حواسيب العالم اجمع .

مشكلات البحث :

في حلول العام ١٩٩٠ تزايد حجم المشكلة بشكل ملحوظ فظهرت الحاجة الملحة لوجود برنامج مضاد للفيروسات ، فكان أول برنامج من هذا النوع هو البرنامج المعروف باسم " Norton Anti Virus **" الذي أصدرته شركة "** Symantec **" عام ١٩٩٠ .**

ومع ظهور طريقة جديدة لاكتشاف الفيروسات و التخلص منها أصبحت الفيروسات بحاجة ملحة لرماز أكثر تطورا يمكنها من القفز فوق البرمجيات المضادة لها فظهرت الفيروسات متعددة الأشكال في العام ١٩٩١ .

ومع ظهور نظام التشغيل windows 95 اعتقد العديدون أن الفيروسات إلى زوال ، لكن ما حدث بالفعل ظهور فيروسات أكثر خبثا وضررا عرفت باسم فيروسات المايكرو ، وفي العام ٢٠٠٠ أصبح بإمكان الفيروسات أن تنتشر عبر شبكة الانترنت عن طريق الالتصاق برسائل البريد الالكتروني وغيرها من الكائنات التي تنقلها الشبكة .

يبقى السؤال الأهم هو : من يكتب تلك الفيروسات وما الذي يدفع مبرمج ذكي إلى كتابة برامج تتسلل إلى أنظمة الآخرين وتحاول إيذائها ؟

لقد طرح هذا السؤال في عدد كبير من المقالات وكتب المعلوماتية وحتى الفلاسفة ، ولقد تصدرت Sara Cordo الخبيرة بالبرامج المضادة للفيروسات لدراسة هذا الموضوع بعمق .

الفصل الثاني

(ماهية الفيروسات وسبل مهاجمتها للحواسيب)

- **تعريف الفيروس:**

يعرف فيروس الحاسوب بأنه برنامج ينفذ وينسخ نفسه دون معرفة (المضيف) أي المستخدم هنا، ومع إن الفيروسات ليست مدمرة بالضرورة لكن يمكن ان يقوم بعضها بإتلاف الملفات أو الكتابة فوقها أو بأعمال مؤذية أخرى.

ويوصف الفيروس عموما كما يلي:

1. **هو برنامج قادر على التكاثر، أي يستطيع أن ينشئ نسخا من ذاته (ليست بالضرورة متطابقة).**
2. **تعتبر عملية النسخ الذاتي غاية بحد ذاتها وليست مجرد اثر جانبي لفعل آخر.**
3. **بعض النسخ المولدة (على الأقل) هي فيروسات أيضا وفق هذا التوصيف.**
4. **يلتصق الفيروس بمضيف ما بحيث يؤدي تنفيذ المضيف إلى تنفيذ الفيروس .**

- **بنية الفيروس ومكوناته الوظيفية:**

يتضمن أي فيروس إجرائيتين أساسيتين لا غنى عنهما، الأولى هي إجرائية البحث التي تقوم بتحديد الملفات أو مواقع الذاكرة التي يمكن أن تكون هدفا للفيروس، تقوم هذه الإجرائية إذا بتحديد الموقع الذي ستتم عملية نسخ الفيروس إليه كما تحدد إذا كان يجب أن يتم هذا النسخ بسرعة أم ببطء، وإذا كان بإمكان الفيروس مهاجمة وحدات مختلفة داخل الحاســوب أم القرص الصلب فقط مثلا، وإذا كان بإمكانه مهاجمة أي جزء من القرص أم أجزاء محددة منه.

يمكن أن يكون برنامج البحث هذا متطورا إلا إن ذلك يتطلب استخدام المزيد من الذاكرة لتخزين تعليمات الفيروس، وبالرغم من إن طريقة البحث أكثر كفاءة يمكنها أن

تساعد الفيروس على تأدية عمله بشكل أفضل إلا أن ذلك سيؤدي إلى زيادة حجم الفيروس وهذا آمر غير مرغوب فيه من وجهة نظر كاتب الفيروس.

أما الإجرائية الأخرى التي يجب أن يتضمنها الفيروس فهي إجرائية النسخ التي تقوم بإعادة نسخ تعليمات الفيروس إلى المنطقة التي تكوون إجرائية البحث قد حددتها في وقت سابق، ويجب أن تكون هذه الإجرائية متطورة بما يكفي لان تؤدي عملها دون أن تصبح عرضة للاكتشاف، وكلما كانت هذه الإجرائية صغيرة كلما كان أداء الفيروس أفضل، ويرتبط حجم هذه الإجرائية عادة بدرجة تعقيد آلية النسخ، فالفيروس المصمم لمهاجمة ملفات com فقط يستخدم إجرائية نسخ اصغر بكثير من تلك التي يستخدمها الفيروس المصمم لمهاجمة ملفات EXE ،إذ إن صيغة الملف EXE أكثر تعقيدا من صيغة الملف com وبالتالي يحتاج الفيروس لمزيد من العمل لكي يستطيع الالتصاق بالملفات من نوع EXE .

تسمح هاتان الإجرائيتان للفيروس بتنفيذ أهدافه، إلا انه قد يضاف للفيروس في بعض الأحيان وظيفة أخرى بهدف حمايته، أي إخفائه بحيث يصعب على المستخدم أو برامج البحث عن الفيروسات اكتشاف وجوده، ويمكن تحقيق هذه الوظيفة ضمن إجرائيتي البحث والنسخ، كما يمكن إن تشكل إجرائية مستقلة بحد ذاتها. يمكن لبرنامج البحث مثلا أن يقصر عمله على منطقة صغيرة محددة وذلك أن ترك هذا البرنامج يعمل دون قيود قد ينبه المستخدم بطريقة أو بأخرى إلى حدوث فعالية غير عادية ضمن الحاسوب. من ناحية أخرى يمكن لبرنامج الإخفاء أن يضبط عمل الفيروس، فعلى سبيل المثال يمكن أن يقوم هذا البرنامج بإطلاق عمل الفيروس في وقت وتاريخ محددين يكون الفيروس قبله هامدا، أو يطلق عمله عند غياب الضغط على احد المفاتيح لمدة خمس دقائق مثلا، الأمر الذي يعني إن المستخدم غائب عن مراقبة حاسوبه.

تشكل الاجرائيات الثلاث السابقة المكونات الضرورية لعمل الفيروس وسوف نقوم بدراستها بالتفصيل خلال هذا الكتاب. وقد تتضمن بعض الفيروسات اجرائيات أخرى غير تلك المذكورة هنا، إذ يمكن أن يتضمن الفيروس اجرائيات أخرى تهدف إلى تعطيل عمل الحاسوب كليا، وأحيانا تخريبه فيزيائيا، وأحيانا أخرى للعب والتسلية فقط.

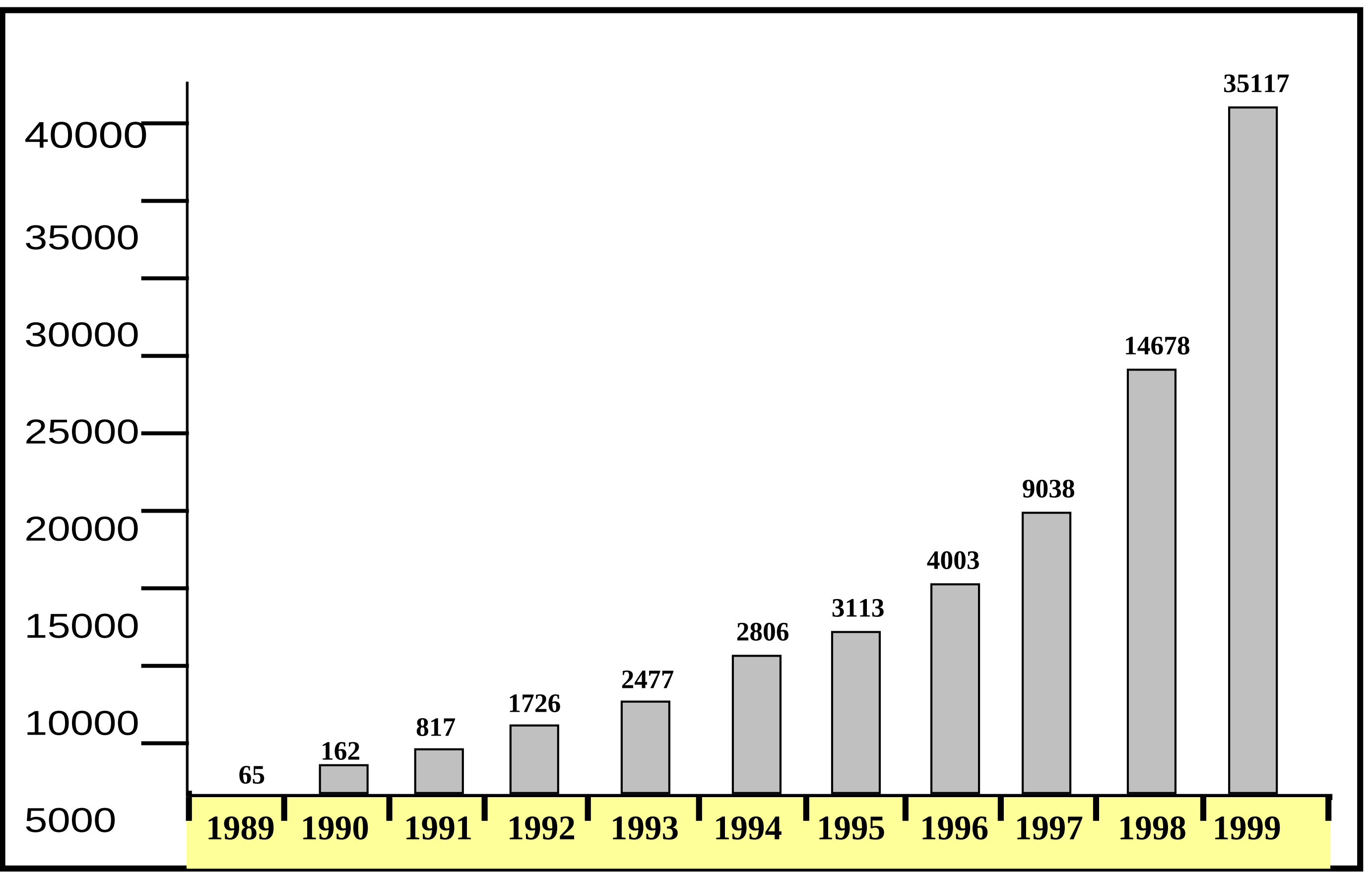
لا تعتبر هذه الاجرائيات الإضافية أساسية لعمل الفيروس، بل على العكس فهي ضارة بالفيروس نفسه أحيانا، إذ يمكن أن تجذب انتباه المستخدم لوجوده.

إن معظم الفيروسات الشائعة هي فيروسات (انتحارية) يتم اكتشافها فورا بعد تنفيذها، وهي لا تكتب بهدف التدمير وتخريب المعلومات بل بهدف اللهو واللعب فقط، فقد صمم احد الفيروسات مثلا بحيث يجعل الحاسوب يبدو كما لو انه آلة غسيل فتظهر شاشته بعض الرسوم العشوائية ويصدر ضجيجا يشبه آلة الغسيل.

ما هو الحجم الحقيقي لمشكلة الفيروسات؟

أعلنت شركات Network Associates التي وضعـــت البرنامج Virus Scan المضاد للفيروسات إنها رصدت أكثر من (00 570) برنامج مؤذي، ومع إن هذا العدد اكبر من كل الأعداد التي أعلنتها الشركات الأخرى التي تعمل في مجال كتابة البرامج المضادة للفيروسات فمن المؤكد أن العدد الفعلي للفيروسات يتراوح بين 3500 و 5000 فيروسا. وتشير بعض الاستطلاعات إلى إن أكثر من 98% من شركات الأعمال في أمريكا الشمالية تتعرض سنويا لمشكلات ناجمة عن الفيروسات والبرامج المؤذية الأخرى.

وتقدر تكاليف الأضرار الناجمة عنها بين 1 و 3 كما أعلن المركز Trend Micro المتخصص بتعقب الفيروسات، إن أكثر من مليون إصابة تحدث كل يوم. والشكل الآتي يبين التزايد لعدد الفيروسات منذ بدء ظهورها وحتى نهاية القرن الماضي حيث آخذنا القيم الوسطى للأعداد التي أعلنتها بعض الشركات الموردة للبرامج المضادة للفيروسات.



السنة

وقد أعلن مخبر الجمعية لأمن الحواسيب انه توصل من خلال دراسة أجراها في العام 2000 إلى مجموعة الحقائق التالية:

- من بين كل 1000 حاسوب مشمول بالدراسة يتعرض 160 حاسوب كل عام للإصابة بالفيروسات.
- تعرض أكثر من نصف مراكز الأعمال المشمولة إلى كارثة تسببها الفيروسات (إصابة أكثر من 25 حاسوب في الوقت نفسه) .
- يبلغ الزمن الوسطي لتوقف العمل الناجم عن الفيروسات حوالي 21 ساعة لكل حاسوب سنويا.
- تعرض أكثر من 80% من مراكز الأعمال إلى كوارث بسبب الفيروسات الواردة عن طريق البريد الالكتروني.

- **يستخدم أكثر من 68% من المراكز المشمولة بالدراسة برمجيات مضادة للفيروسات.**

- **إن أهم ما تجدر ملاحظته من نتائج هذه الدراسة هو عدم كفاية البرامج المضادة للفيروسات للحماية منها.**

ما هي الأضرار التي يمكن أن يسببها الفيروس؟

لا تسبب معظم الفيروسات أضرارا جدية على الإطلاق. في حين يمكن أن تتسبب بعض الفيروسات بأشكال متنوعة جدا من الإزعاجات أو الأضرار الجدية، وإذا كانت كل الفيروسات تشغل حيزا من مناطق التخزين المتوفرة وتشغل موارد النظام إلا أن بعضها قد يسبب ما يلي:

- **اختناقات في خدمات البريد الالكتروني.**
- **حذف الملفات أو تعديلها.**
- **إفشاء معلومات أو أسرار شخصية هامة.**
- **تخفيض مستوى أداء الحاسوب.**
- **تخفيض إنتاجية الحاسوب والمستخدم.**
- **إظهار رسائل جدية أو ساخرة على الشاشة.**
- **حذف محتويات الملفات.**
- **تشويه المعطيات.**
- **توليد سلوك غريب يؤدي إلى إيقاف الحاسوب.**
- **توليد إشارات صوتية مزعجة أو توليد موسيقى عادية .**
- **إيذاء البرمجيات التطبيقية.**

وبصيغة أخرى قد تكون الاضرار الناجمة عن وجود الفيروسات:

- **محدودة: يكون اثر الفيروس مقتصرا على إزعاج المستخدم دون إيذاء البرامج أو الملفات، وتكون إزالة الفيروس سهلة كما يمكن إصلاح آثاره بسهولة أيضا. يؤدي**

الفيروس Form مثلا إلى إصدار الصوت العادي (Beep) عند الضغط على مفاتيح لوحة المفاتيح في اليوم الثامن عشر من الشهر.

- متوسطة: كأن يتسبب الفيروس في تعطيل بعض البرامج التطبيقية مما قد يضطرك إلى إعادة تثبيتها من جديد.

- شديدة: كأن يتسبب الفيروس بتهيئة سواقة القرص الصلب أو الكتابة فوقها، كما يفعل الفيروس Michelangelo الذي ينشط في السادس من آذار وهو تاريخ ولادة الفنان Michelangelo Bounnaroti فيكتب معطيات غير مفيدة فوق القسم الأكبر من القرص الصلب.

- كتابة الفيروسات:

كتبت معظم الفيروسات فيما مضى باللغة التجميعية Assembly Language لكن يمكن من حيث المبدأ أن تكتب الفيروسات بلغة عالية المستوى مثل C أو Java أو غيرها، لكن لا توفر هذه اللغات الإمكانيات التي توفرها اللغة التجميعية، فهي اللغة الوحيدة التي تمكننا من السيطرة على كافة موارد الحاسوب واستخدامها بالطريقة التي نريد.

يحتاج تعلم اللغة التجميعية إلى وقت لا بأس به، كما يتطلب معرفة بعض المعلومات المتعلقة ببنيان الحاسوب.

بينما يمكن تعلم اللغات عالية المستوى في وقت اقصر نسبيا ويمكن تعلم لغات الماكرو في وقت قصير جدا، وقد استخدمت هذه اللغات بالفعل لكتابة عدد لا بأس به من الفيروسات، ربما تشكل اليوم القسم الأكبر من الفيروسات المنتشرة عبر العالم، فقد أفسحت هذه اللغات المجال لعدد كبير من الهواة لكتابة الفيروسات الماكرو الخبيثة.

- أعراض الإصابة بالفيروس:

- **تكرار رسائل الخطأ في أكثر من برنامج.**
- **ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.**
- **تكرار اختفاء بعض الملفات التنفيذية.**
- **حدوث بطء شديد في إقلاع نظام التشغيل أو تنفيذ بعض التطبيقات.**

فالفيروس عبارة عن برنامج صمم لينشر نفسه بين الملفات ويندمج أو يلتصق بالبرنامج، فعند تشغيل البرنامج المصاب فانه قد يصيب باقي الملفات الموجودة معه في القرص الصلب أو المرن لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينشر.

لماذا يخلق الناس فيروسات الحاسوب؟

فيروسات الحاسوب لا تتشابه في وجودها بالفيروسات الحيوية. إن فيروس الحاسوب لا ينشئ من لا شيء أو لا يأتي من مصدر مجهول أو ينشئ بسبب خلل بسيط في الحاسوب. فيروس الحاسوب يتم برمجته من قبل المبرمجين أو الشركات ويتم صنعه بشكل متعمد ويتم تصميمه بشكل متقن. يعمل المبرمجون على خلق الفيروسات وذلك لأهداف عديدة تتنوع من اقتصادية وسياسية وتجارية وعسكرية. فبعض المبرمجين يعتبرون إن عمل الفيروس نوع من الفن والهواية التي يمارسونها. ومن أهم الأهداف لعمل فيروس الحاسوب هو الهدف التجاري. ذلك عن طريق عمل وصنع الفيروسات من اجل بيع برامج مضادات الفيروسات. يذكر إن المبرمج الذي يعمل الفيروس يعتبر حسب القانون مجرما وصناعة الفيروس جريمة يحاسب عليها قانون الدولة الموجود بها. معظم شركات مضادات الفيروسات تقوم بصناعة الفيروسات من قبل المبرمجين تقوم بعمل مضادات لها وذلك لتسويق منتجاتها وبرامجها لدى مستخدمي الكومبيوتر برنامج تطفلي تخريبي يقحم نفسه في ملفات الحاسوب عبر عملية نسخ نفسه. ويتم عادة تنفيذ الفيروسات عند تحميل الملفات المصابة إلى الذاكرة مما يسمح بإعادة عملية انسخ.. الأثر السلبي للفيروسات واضح دائما ومن الممكن أن يكون تأثيرها عالميا.احد الأمور التي قد يقوم بها الفيروس هي حجز مكان كبير من الذاكرة وبالتالي عدم السماح للبرامج بأخذ مكانها المطلوب.

تدعى البرامج التي تمتلك القدرة على نسخ نفسها والانتهاء بنتائج مؤذية على الحاسوب بالبكتريا bacterium .

الفصل الثالث

الفيروسات وكيفية مهاجمتها للنظام DOS والنظام WINDOWS

تمهيد:

إن الانتشار الكبير للحواسيب الشخصية المترافقة مع حواسيب IBM والتي تستخدم معالجات (Intel) وتشغل برامج مخصصة للعمل ضمن بيئة نظام DOS قد ساعد كثيرا في توسيع الوسط الذي ينتشر فيه الرماز النقال المؤذي وعلى الرغم من انتشار واستخدام نظام التشغيل WINDOWS في السنوات العشر الأخيرة مازال الكثيرون يعتبرون فيروسات النظام DOS نموذجا أساسيا للرماز النقال المؤذي، وذلك نظرا لكثرتها. وبذلك نعتقد إن فهم آلية عمل هذه الفيروسات ضروري لفهم آلية عمل الرماز النقال المؤذي.

- **الملفات التنفيذية** EXE و COM

إن كتابة وتعديل الملفات COM أسهل من كتابة وتعديل الملفات EXE لكنها تخضع بالمقابل لقيد بنيوي إذ يمكن أن يتجاوز حجمها 4KB وتخزين المعطيات الخاصة بالبرنامج مع البرنامج نفسه في مقطع واحد من الذاكرة حجمه 4KB. يمكن إنشاء برامج اكبر باستخدام تقنية تراكب الملفات وتبديل أجزاء البرامج الموجودة في الذاكرة وهذا يفسر سهولة مهاجمة الفيروسات للملفات المتراكبة (OVL).

يطابق ملف COM الموجود في الذاكرة النسخة الرقمية الثنائية الموجودة على القرص باستثناء وحيد، فكما يبين الشكل التالي لكل ملف COM ترويسة طولها 256 بايت تسمى بادئة مقطع البرنامج PSP

(Program Segment Prefix) التي يعدها نظام DOS دون العودة إلى الملف الأصلي.

الرماز، المعطيات، المكدس (64 KB)	الترويسة PSP بادئة مقطع البرنامج

بنية الملف COM

الملفات EXE :

يختلف الملف EXE المشحون إلى الذاكرة عن صورته الثنائية الموجودة على القرص، إذ يمكن أن يشغل اكبر عدد من المقاطع، وتوضع المعطيات في مقاطع غير تلك التي توضع فيها تعليمات البرنامج، ويهتم النظام DOS بإعداد بادئة مقطع البرنامج (PSP) لكنه يستقي المعلومات الأخرى من ترويسة الملف EXE التي يبلغ طولها 512 بايت والتي تحوي معلومات تخبر نظام DOS أين توضع المقاطع المختلفة (مقطع الرماز ومقطع المعطيات ومقطع المكدس) وأين يبدأ رماز البرنامج ، والشكل التالي يبين الملف EXE

مقاطع المكدس (64 KB)	**مقاطع المعطيات** (64 KB)	**مقاطع الرماز** (64 KB)	**الترويسة**

بنية الملف EXE

فيروسات الملفات:

تستخدم فيروسات الحاسوب رماز الملفات المضيفة لكي تنشر فيكتب فيروس الملف رمازه نفسه على الملفات المضيفة الأخرى التي تكون عادة ملفات تنفيذية كملفات COM **أو كملفات** EXE **، وقد تكون أيضا ملفات معطيات أو ملفات** SYS **أو** DLL **أو** OBI **ويمكن تصنيف فيروسات الملفات في ثلاث فئات: الأول لا يحل فيها الفيروس رمازه محل رماز الملف المصاب. والثانية يتصل فيها الفيروس بالملف المصاب. والثالثة يبقى فيها الفيروس مرافقا للملف.**

الفيروسات التي تتصل بالملف المضيف Appending Viruses:

تضيف فيروسات هذا النوع رمازها إلى الملف المضيف الأصلي دون أن تدمره ويضيف بعضها رمازه إلى نهاية الملف المضيف (Appending) **بينما يضيف بعضها الأخر رمازه إلى بداية الملف المضيف** (Prepending) **لكن على هذه الفيروسات أن تحدد أولا نمط الملفات المضيفة التي ستهاجمها، فلكل نمط من الملفات** COM **أو** EXE **أو** SYS **أو غيرها، بنيته الخاصة التي يجب الحفظ عليها بعد إضافة رماز الفيروس وتعتبر هذه الفيروسات أكثر قدرة على النجاح والانتشار لأنها تحافظ على الوظيفة الأصلية للملف**

المضيف فيتأخر اكتشاف وجودها. ونشير هنا إلى أن تنفيذ رماز الفيروس لن يزيد على زمن تنفيذ الملف السليم إلا أجزاء صغيرة من الثانية.

يبين الشكل الآتي مثالا لإصابة ملف بفيروس يضيف رمازه إلى بداية الملف المضيف:

قبل الإصابة

ملف البرنامج الأصلي	**الترويسة**

بعد الإصابة

ملف البرنامج الأصلي	**رماز الفيروس**	**الترويسة**

تمثيل برنامج قبل الإصابة بالفيروس وبعد الإصابة به

إصابة الملفات:

بعد أن يعثر الفيروس {(Espawn) (هو اسم لفيروس يصيب الملفات)} على من يصيبه ينشئ نسخة من تعليماته ذاتها باسم يطابق اسم الملف المضيف لكن مع اللاحقة COM بدلا من اللاحقة EXE ، ولإعادة تسمية المضيف ينسخ الفيروس اسمه في المنطقة DTA حيث وضعته إجرائية البحث، ويحفظ هذا الاسم في المتحول COM ثم ينشئ Espawn ملفا بالاسم الأصلي للمضيف.

```
MOV   ah , 9EH              ;DTA+1EH, Com File Name
MOV   ah , 3CH              ;DOS File Create Function
MOV   cx , 2                ;hidden attibute
MT    21H
```

ثم يكتب نسخة من رمازه في هذا الملف:

```
MOV   ah , 4OH              ;DOS File Write Function
MOV  CX ,Finish-Espawn      ;Size of Virus
MOV   dx , 100 H            ;Location of Virus
Int    21 H
```

نلاحظ هنا كيف يعطي الفيروس Espawn الصفة (مخفي) للملف الذي ينشئه وبذلك يصبح العثور عليه أصعب.

الفيروسات وأنظمة WINDOWS :

تقانات WINDOWS

بدأ نظام Microsoft Winowdos **كغلاف يخفي خشونة نظام** DOS **ثم بدأ يقل اعتماده على هذا النظام تدريجيا، وقد وضعت شركة ميكروسوفت نواتين مختلفتين لمنصات عمل** WINDOWS 9X **و** NT**. ومع إنهما تبدوان متشابهتان لكنهما في العمل مختلفتان بشكل واضح. ونشير هنا إلى إن نظام** Windows ME **ينتمي إلى الفئة** 9X **بينما ينتمي نظام** Windows 2000 **إلى الفئة** NT.

تعتبر كتابة التطبيقات لأي من المنصتين أصعب بكثير من كتابة تطبيقات النظام DOS **، ولذلك تأخرت فيروسات نظام** WINDOWS **بالظهور بعد عدة سنوات من انتشاره مما جعل الكثيرين يعتقدون انه قد قضي على فيروسات الحاسوب ليتبين لاحقا إن هذا الاعتقاد كان خاطئا.**

تستخدم إصدارات WINDOWS**الحالية الكثير من المبادئ والتقانات التي قدمتها شركة ميكروسوفت** WINDOWS 3.X **ولن نتعرض في الفقرات القادمة إلا للتقانات والمفاهيم التي تهمنا لدراسة عمل الفيروسات او الرماز النقال المؤذي، لذلك قد تبدو هذه الفقرات غير مترابطة لكنها تقدم ما يكفي لموضوعها الحالي.**

فيروسات النظام WINDOWS على منصات عمل WINDOWS :

كان الفيروس Win Vir أول فيروس مخصص لمهاجمة بيئة النظام WINDOWS ، وقد ظهر هذا الفيروس في نيسان من العام 1992 أي بعد عامين من صدور النظام WINDOWS 3.0 . ومع انه كان يصيب ملفات EXE التنفيذية لكنه لم يكن يحوي أي استدعاء لتوابع الواجهة API (Application Program Interface) بل كان يعتمد على مقاطعات النظام DOS . يصيب هذا الفيروس عند تشغيله كل الملفات EXE الموجودة في الدليل الحالي ويحذف رمازه من البرنامج الذي يستضيفه.

وفي شباط من العام 1996 ظهر الفيروس Boza وهو أول فيروس مخصص للعمل في بيئة النظام WINDOWS 95 ، يبحث هذا الفيروس عند تشغيله عن ثلاثة ملفات تنفيذية من النمط 32- بت في الدليل الحالي ليصيبها ، وإذا لم يعثر على ثلاثة ملفات ينتقل للبحث في الدليل ذي المستوى الأعلى مباشرة.وبالتالي فقد يصل إلى الدليل الجذري . وفي اليوم الثلاثين من كل شهر يعرض الفيروس Boza رسالة تعرض عن وجود وتعرض قائمة بفيروسات أخرى كتبتها المجموعة المعروفة باسم VLDA.

لم يعد من الضروري استخدام اللغة التجميعية لكتابة فيروسات النظام WINDOWS ، فقد سهلت لغات البرمجة عالية المستوى التي تطورت مع ظهور هذا النظام كتابة الفيروسات ، كما أصبحت بنى الملفات الموثقة بشكل أفضل وأصبح من السهل العثور على الوثائق مجانا على شبكة الويب.

أمثلة من فيروسات نظام WINDOWS :

الفيروس Win 32.Kri2 :

يصيب الفيروس Kir2 **ملفات** PE **التنفيذية ، وهو يحاول أن يسبب أذى مشابها لما يسببه الفيروس** CIH **ولكن في** 25 **كانون الأول من كل عام . لكنه لا ينجح إلا على أنظمة** WINDOWS 9X .

عند تشغيله للمرة الأولى ينسخ هذا الفيروس نفسه إلى ملف اسمه KRZIED.TT6 **ثم يعدل أو ينشئ ملف** WININIT.INI **بحيث يجري نسخ هذا الملف فوق الملف** KERNEL32.DLL **عند الإقلاع التالي وهو يصيب ملفات تنفيذية متنوعة عند استدعاء توابع معينة من الواجهة** API .

الفيروس Win95.Prizzy :

كتبه مبرمج تشيكي اسمه Prizzy **محاولا تجاوز حدود فيروسات النظام** WINDOWS **، فكان الفيروس** Prizzy **أول فيروس يستخدم تعليمات المعالج الحسابي المساعد الذي كان في الحواسيب الأولى عبارة عن رقاقة مستقلة. لكن بعد ظهور الجيل** 486 **أصبح جزئا من المعالج نفسه. يحاول المعالج الحسابي المساعد تخفيف أعباء المعالج بانجاز العمليات الحسابية المعقدة . ثم قدمت رقاقات** Pentium **معالجا مساعدا جديدا سمي** mmx (multimedia exetension) **لتسريع عمليات الرسم البياني المعقدة . وقد وجدت الفيروسات متعددة الأشكال في استخدام تعليمات المعالج المساعد وسيلة جيدة إذ يؤدي استخدام هذه التعليمات إلى زيادة صعوبة اكتشاف الفيروس . ومع إن الفيروس** Prizzy **لم يكن ناجحا لكنه مهد الطريق لظهور فيروسات جديدة تستخدم تعليمات المعالج المساعد نذكر منها الفيروس** Win32.Thorin **والفيروس** Win32.Legacy .

الفيروسات والانترنيت

لا يمكن اعتبار أي حاسوب متصل بشبكة الانترنت آمنا تماما ، إذ مهما اتخذ من إجراءات يبقى برنامج التصفح معقدا بحيث لا يمكنك سد كل الثغرات ، وإذا كنا نريد أمانا مطلقا فما علينا إلا حذف المصفح .

قد نستغرب هذا القول ، لكن بالفعل فمجرد التجول عبر الشبكة يعرض الحاسوب للخطر ، فعند الوصول إلى صفحة الويب يجري عادة تحميل كل محتوياتها التي يسمح لنا بتحميلها . وقد تكون بعض هذه المحتويات قالبة للتنفيذ ، ويمتلك المبرمج ترسانة من الأدوات التي تستطيع أن تحول ارتباطا بسيطا إلى كائن مؤذ عبر استخدام التقانات التالية :

- لغة HTML .
- اللغات الخطاطية (مثل Java Script).
- لغة جافا (Java) .
- العناصر Activex
- ملحقات المتصفح (browser add-ons) .

لغة HTML :

إن وثائق الويب هو عبارة عن الملفات نصية عادية تخضع لمعايير لغة تأشير النصوص الفائقة

HTM(Hyper Text Mar Kup Language) التي تعتبر بدورها مجموعة جزئية من لغة أوسع كانت تستخدم لتوصيف الوثائق قبل HTML هي لغة SGML

(Standarzid Ganeral Mar Kup Laguage) .

ويضم ملف HTML البسيط أربعة مكونات وهي :

- النصوص .
- الإمارات (Tags) .

- **الارتباطات** (Links) .
- **محتويات أخرى غير نصية.**

ويمكننا أن نعطي مثال لوثيقة HTML **الصغيرة** .

```
<HTML>
<HEAD>
<TITLE>Tiny HMTL document</TITLE>
<BODY>
<P>Hello Word !
</BODY>
</HMTL>
```

يمثل نص برمجي لوثيقة HMTL **صغيرة .**

أما هذا الجدول فيمثل بعض امارات HMTL **التي يمكن استغلالها لنقل الفيروسات والرماز المؤذي:**

الامارة	الوصف	مثال

<Img.Scr>	تشير إلى صورة ضمن وثيقة الوب	<Img.Scr="graphics/picture.gif "> **تحمل ملفا بيانيا اسمه** picture.gif **من الدليل الفرعي** graphics **من مخدم الوب ضمن المتصفح .**
<Aherf>	لإنشاء ارتباط بوثيقة أخرى أو بغرض آخر	<a herf= http://www.myexample.com/index.html>
<Frameset>	لتعريف خصائص وحدود مجموعة من الأطارات ضمن المتصفح .	<Frameset Cols=" 50% ,50% " rows=" 75% , 25% ">
<script>	لتعريف موقع خطاطة في الصفحة	<script Type= "text/vbscript" scr = "hppt//www.example.com/vbcale"> </SCRIPT>

بعض إمارات HMTL **التي يمكن استغلاها لنقل الفيروسات والرماز المؤذي.**

– بعض التقانات :

لقد أدى الانتشار الكبير الذي لاقته برامج تصفح الانترنت تطور هذه البرامج وزيادة تعقيدها بحيث أصبحت وظائفها كثيرة ومتشبعة ، وبحيث ازدادت الصلات بين هذه البرامج وكل أنواع البرامج الأخرى ، مما أدى بدوره إلى فتح أفاق جديدة كثيرة

للقراصنة وكاتبي الفيروسات ، وسنستعرض فيما يلي بعض التقانات التي يمكن لكاتبي الفيروسات استغلالها.

– مواضيع السرية والخصوصية :

يتساءل المستخدمون دوما عما يمكن لموقع الوب أن يعرفه عنهم من معلومات شخصية بمجرد زيارته . تمتلك مواقع الوب أربع طرق لجمع المعلومات :–

- معلومات عامة من المتصفح .
- المعلومات التي يدخلها المستخدم في الاستمارات.
- تقنيات التعقب .
- الكعكات (Cookies) .

- الكعكات (Cookies) :

وهي ملفات نصية ينشئها موقع الوب ويخزنها على القرص الصلب المحلي (عادة في الدليل winder%cookies%) ويستخدمها لتساعده في تذكر معلومات عن زيارتك ، وعند إنشاء كل كعكة يخزن سجل موافق في ملف (هو الملف INDEX.DAT في Internt Explorer) .

يمكن أن تكون الكعكات دائمة (تحفظ من زيارة لاخرى) وقد تكون صالحة من خلال جلسة العمل الحالية فقط ، كما يمكن أن يولد موقع الويب الحالي الكعكات ويستخدمها بنفسه ،. وقد يولدها ليستخدمها موقع آخر ، فقد يولدها موقع لشركة استشارية ليتم الوصول إليها كلما انتقل المستخدم إلى موقع ويب عبر الأشرطة الإعلانية التي تظهر على موقع الشركة .

لا تشكل الكعكات خطرا هاما على النظام فهي مقيدة بما يكفي أن تعرفه عنك دون سؤالك ويخشى بعض الناس من أن تستخدمها المواقع للبحث في أقراصهم المحلية أو قراءة معلومات عن حساباتهم المصرفية وتسجل ما يقومون به من أنشطة ، لكن الكعكات ليست ملائمة لهذه وتسمح لك معظم المتصفحات بإبطال إمكانية إنشاء واستخدام الكعكات لكن استخدامها أصبح شائعا لدرجة إن العديد من المواقع لن تعمل بدونها .

متى يجب أن تثير محتويات المتصفح قلق المستخدم :

تصبح محتويات المتصفح خطيرة إذا كان بإمكانها القيام بأي من الأفعال التالية :

- الوصول إلى موارد الحاسوب والملفات المحلية .
- التشغيل التلقائي على الآلة المحلية دون ترخيص المستخدم .
- البقاء في الذاكرة دون تنبيه المستخدم .
- التعامل مع البرامج الخارجية الموجودة على الآلة المحلية .
- الوصول إلى نوافذ المتصفح الأخرى والتعامل معها .
- إطلاق إجراءات جديدة على الآلة المحلية .

فيروسات البريد الالكتروني :

تستطيع رسائل البريد الالكتروني أن تصل إلى آلاف المستخدمين ، إن لم نقل الملايين بسرعة الضوء لتجوب كوكب الأرض خلال وقت قصير ولذلك أصبحت الرسائل وسيلة فعالة لنقل الفيروسات ونشرها .

كان استخدام ملفات الارتباط (attachment) الوسيلة الوحيدة لنشر الفيروسات على البريد الالكتروني خلال السنوات الأولى لظهوره ، إذ كان على المستخدم أن يفتح أو يشغل ملف الارتباط لتنفيذ الرماز ، ومازالت هذه الطريقة حتى الآن الطريقة الأكثر شيوعا لكنها لم تعد الوحيدة إذ أصبح بالإمكان تصفيف ماكروات ورماز تنفيذي وأغراض

Activex في الرسالة نفسها ، ويستطيع زبون البريد الالكتروني أن ينفذ الرماز دون طلب المستخدم .

برامج البريد الالكتروني :

يتواجد في الأسواق اليوم العديد من برامج البريد الالكتروني الهامة ، وقد كتبت معظم الفيروسات وبرامج القرصنة لتخترق تحديدا البرنامج Microsoft Outlook ، لكن يمكنها أن تنجح بدرجات مختلفة على معظم برامج البريد الالكتروني الشائعة الاستخدام .

أنماط البريد الالكتروني :

يمكن تصنيف برمجيات البريد الالكتروني في ثلاث فئات أساسية :

- زبون / مخدم (Client / server) .
- برمجيات معتمدة على الوب (Web-based) .
- برمجيات معتمدة على الاستضافة (Host-based) .

إن النمط الأكثر انتشارا اليوم هو الذي يعتمد على نموذج الزبون / المخدم إذ يتبضع برنامج البريد الرئيسي على حاسوب الزبون المحلي ويتصل بقاعدة معطيات مخدم بريد رئيسي لإرسال وتلقي الرسائل ، حيث يجمع هذا المخدم كل الرسائل ويوزعها أما إلى الزبائن وأما إلى مخدمات بريد الكتروني أخرى ليعاد توجيهها إلى وجهاتها . ومن أشهر البرامج التي تعتمد على هذا النموذج :

Netscape Messenger Microsoft Outlook
و Microsoft Exchange

تسمح أنظمة البريد الالكتروني المعتمدة على الويب مثل Hot Mail أو Yahoo Mail للمستخدمين النهائيين بتلقي رسائل البريد الالكتروني من أي حاسوب يحوي متصفح متصل بالانترنت ، إذ يجب على المستخدم أن يدخل اسم حساب البريد وكلمة

مرور من خلال صفحة HTML عادية ، ولذلك تسمح معظم هذه الأنظمة بإدراج الخطاطات ضمن نص رسالة وإرسالها إلى مستخدم الوجهة . وتم تسجيل العديد من حالات الاختراق لهذه الأنظمة المعتمدة على الوب ، لكن تتمتع هذه الأنظمة من ناحية أخرى ببعض المزايا الأمنية إذ تخزن الرسائل عل مخدم بريد الكتروني بعيد وتستخدم لنقلها بروتوكولات خاصة ، ولذلك لن تستطيع العديد من الفيروسات أن تصل إلى حاسوب الزبون .

أما أنظمة البريد الالكتروني المعتمدة على الاستضافة فلم تعد مستخدمة على نطاق واسع اليوم إلا في الشركات الكبيرة . وفي هذه الأنظمة تخزن برمجيات الزبون والمخدم على الحاسوب نفسه ، وهي الأنظمة الأكثر أمانا.

ديدان البريد الالكتروني :

لم يتطلب انتشار الفيروس Melissa عبر العالم ألا أياما قليلة ، ومنذ ذلك الوقت أدرك الجميع إن فيروسات أو ديدان البريد الالكتروني باتت تشكل خطرا جديا على الحواسيب المنتشرة في العالم ، ولا تقتصر مقدرة ها النوع من الفيروسات على الانتشار عبر العالم خلال ساعات بل هي تستطيع تعديل أو إذابة كل ملفات الحاسوب أو الشبكة خلال الفترة نفسها ، إذ قبل أن يدرك مدير الشبكة المحلية وجود خطأ ما يكون الفيروس قد أرسل آلاف الرسائل واتلف عشرات آلاف من الملفات .

يستطيع كاتبو الفيروسات على عوامل نفسية لمساعدة فيروساتهم على الانتشار ، فالفيروس I Love You مثلا موجه للجميع ، بينما هاجم الفيروس Melissa مرتادي المواقع الإباحية ، بل حتى هناك فيروس اسمه Pokemon موجه للأطفال .

من أهم الفيروسات هي :

1-Cavity virus

نوع من الفيروسات يدمج ثم يخفي نفسه في جزء من ملف ما ، مما يسمح للفيروس بالبقاء مخبئا ودون أن يؤثر على وظيفة الملف .

2-Worm **دودة**

برنامج يقوم بنسخ نفسه عبر مجموعة من الحواسيب ، ومن الممكن أن تنسخ الدودة نفسها داخل الجهاز نفسه مؤدية إلى انهيار النظام .

3-CIH virus **فيروس شرنوبل**

فيروس على مستوى عالي من التخريب ظهر أول مرة عام 1998 **. يقوم هذا الفيروس بمحاولة الكتابة على ال** Flash BIOS **في الحسب المصاب بحيث يجعل الحاسب غير قابل للإقلاع** (Unbootable) **.**

أطلق عليه اسم شرنوبل بسبب التاريخ الذي تم تفعيل الفيروس فيه لأول مرة وهو ذكرى حادثة المفاعل النووي شرنوبل .

4-Cluster virus

فيروس يصيب برنامجا واحدا فقط في النظام ولكن ما يظهر للمستخدم هو إن جميع البرامج قد تمت إصابتها بالفيروس.

تقنيا يقوم هذا الفيروس بالتعديل على ملفات النظام بحيث يتم تحميل الفيروس عندما يتم تشغيل أي برنامج وبالتالي يظهر للمستخدم بان الفيروس قد أصاب كل الملفات .

5-Marco virus

فيروس مكتوب بأي لغة ماكرو والتي عادة مدموجة بتطبيق ما حيث يتم تفعيل فيروس الماكرو وعند تشغيل أي ملف يفتح بواسطة التطبيق نفسه.

6-Melissa

فيروس ماكرو شهير يصيب ملفات ال Word **في الرسالة يصل إلى المستخدم كرسالة بريد الكتروني مع ملف مرفق يكون عنوانه :**

An Important Messaga From <user name>

حيث يكون user name **هو احد الأشخاص من دفتر العناوين لديك . عند فتح الملف المرفق يقوم الفيروس مباشرة إذا كان** Microsoft Outlook **منصبا بإرسال نفسه إلى أول** 50 **عنوان من دفتر العناوين لديك ، ويقوم الفيروس بالتلاعب بسجلات النظام** System Registry **يصيب الملف** Normal.dot **وهو قالب ملف ال** Word **لأي ملف جديد وبالتالي يضمن الفيروس إصابة أي ملف** Word **جديد به . ربما لا يمتلك** Melissa **آثار تدميرية كبيرة على الجهاز المصاب لكنه يرهق حساب البريد الالكتروني الخاص بك عبر زيادة عدد الرسائل المرسلة إليك مثلا . تم تسمية هذا الفيروس بهذا الاسم بعد معرفة الشخص الذي صممه .**

7-malicious mobile code

فيروس أو برنامج يستفيد من الضعف الموجود في نظام التراسل اللاسلكي . يمكن أن يصيب الحواسيب والأجهزة الكفية والهواتف التي تتمتع بقدرة الدخول إلى الانترنيت أو أي جهاز آخر يعتمد اسلوب التراسل اللاسلكي.

8-Multipartite virus

فيروس يقوم على دمج قدرات نوعين مختلفين من الفيروسات فيروسات ال boot sector وفيروسات الملفات فتقوم هذه الفيروسات بإصابة جزء من ملفات النظام ثم تتوزع لتنتشر على كافة أجزاء النظام. وكنتيجة لقدرات هذا الفيروس فانه من الصعب جدا التخلص منه.

9-VBS/VBSWG virus

اختصار ل Visual Basic Script/Visual Basic Script Worm Generator وهو احد أطقم صناعة الفيروسات Virus Creation Toolkit والتي تتيح لأي كائن صناعة فيروسات بدون أي خبرة عملية بالبرمجة.

10-Virus Signature

جزء من كود فيروس ما يقوم بتمييز الفيروس عن غيره من البرامج لذا فان مضاد الفيروسات يقوم دائما بالبحث عن هذا التوقيع (Signature).

11-benign virus

برنامج عادي يمتلك أي خصائص الفيروس المشهور –التضاعف الذاتي مثلا– ولكنه لا يسبب أي ضرر للنظام الذي يصيبه .

12-Peachy virus

فيروس ظهر عام 2001 محاولا – ولأول مرة في عالم الفيروسات– ان يقوم بالانتشار عبر ملفات ال PDF الكتب الالكترونية التي تحتاج Adope Acrobat Reader يستفيد هذا الفيروس من الخاصية الموجودة في Adobe Acrobat التي تسمح بدمج ملفات عادية ضمن ملفات ال PDF .

13-phage virus

فيروس تدميري يصيب الأجهزة الكفية التي تشغل النظام Palm OS **، يصيب فيروس ال** phage **احد البرامج ضمن النظام** Palm OS **ثم ينتشر ليصيب كافة البرامج الباقية كما يقوم هذا الفيروس بنسخ نفسه في أجهزة أخرى مستفيدا من تقنية** Beam **الموجودة في** Palm OS **والتي تسمح بنشر البرامج عبر الأشعة تحت الحمراء.**

14-SHS virus

أي فيروسات تصيب الحاسب عبر إخفاء ملفات ذات امتداد shs **. تنتشر هذه الفيروسات عادة كملفات مرفقة بالبريد الالكتروني .**

15-sparse infector

نوع من الفيروسات لا يعمل إلا عند شرط معين ويبقى ال sparse infector **مخفيا داخل النظام ولا يشعر به المستخدم إلا عند شرط محدد بشكل رقمي كتاريخ معين أو كتشكيل برنامج ما عدد من المرات .**

16-Zoo virus

فيروس الاختبارات أنواع كهذه من الفيروسات لا تنتشر بين مستخدمي الحاسوب وتكون موجودة دوما في مختبرات الشركات المصنعة لبرامج مضادات الفيروسات .

17-overwriting virus

فيروس يقوم بإزالة كافة المعلومات الأصلية الموجودة على الملف المصاب ، وبالتالي يجعل الملف عديم القيمة .

18-retro virus

فيروس يتبع اسلوب مميزا في التخفي عبر إصابة وتعطيل عمل برنامج مضاد الفيروسات يدعى أيضا

anti-anti-virus

19-Explorer Zip

فيروس تدميري يصيب الأجهزة المزودة بنظام Microsoft Windows **يمكن وصفه بأنه دودة** Worm **و** Trojan **بنفس الوقت.**

20-Bomb

برنامج يتم زرعه في الحاسوب بشكل سري بهدف عطبه وجعله غير قادر على العمل .

21-Back door

يقوم بالدخول إلى نظام أو شبكة ما عبر اختراق نظم الحماية فيه حيث يقوم المبرمجين عادة ببناء برامج ال Back door **بهدف اكتشاف أخطاء نظام ما يعملون على تطويره . غالبا ما يتم تسريبه ونشره بين المخترقين مما يسبب مشكلة في امن النظام ويدعى أيضا** trapdoor .

23-I Love You

أصاب هذا الفيروس الذي عرف فيما بعد باسم فيروس الحب حوالي عشرة ملايين مستخدم خلال اقل من أسبوع من وجوده ، وقد تسبب بأضرار اشد من تلك التي تسبب بها الفيروس Melissa **، وقد أصبح واحدا من أشهر الفيروسات في التاريخ ، وقد تم رصد** 13 **صيغة لهذا الفيروس .**

كتب هذا الفيروس بلغة VB script **وهو ينتشر عبر البريد الالكتروني ، وهو قادر على إصابة مستخدمي النظام** WINDOWS **المثبت لديهم الميزة** Windows Scripting Host .

أي المستخدمين الذين يستعملون البرنامج 5.0 IE على أنظمة win98 و win95 وهو يستخدم التطبيق Outlook express ليرسل نسخا إلى كل عناوين البريد الالكتروني المسجلة في دفتر العناوين Address Book .

يصل الفيروس مع ملف مرتبط بالرسالة يحمل اسمه للاحقة VBS . ويختلف موضوع ومتن الفيروس تبعا لصيغته إذ يوجد أكثر من 13 صيغة مختلفة من هذا الفيروس ، منها مثلا الصيغة التي تظهر كالتالي :

Subject : I Love You
Body : Kindly checkthe attached Love Letter coming from me
Attachment : Love -Letter- From-For-You-TXT-VBS

نلاحظ هنا استخدام الجزء TXT في اسم الملف ، وهي على الأغلب وسيلة لخداع المستخدم عبر إيهامه بان الملف المرتبط ليس إلا ملفا نصيا آمنا بينما هو في الواقع رماز خطير بلغة VB script .

يختبر الفيروس فور تنفيذه قيمة المفتاح التالي في قاعدة سجلات النظام :

HKEY_CURRENT_USER\SOFTWARE\Microsoft\ windows scripting Host\settings\Time out

فإذا كان لهذا المفتاح قيمة موجبة يضع الفيروس القيمة 0 بدلا منها ، أما إذا لم يكن هذا المفتاح موجودا فلا يجري أي تعديل.

23-Trojan Horse حصان طروادة

سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها وهكذا تكون إلية عمل هذا الفيروس حيث يكون مرفقا مع احد البرامج أي يكون جزء من برنامج ما دون أن يعلم المستخدم . فعندما يبدأ البرنامج تنفيذ عمله ويصل إلى مرحلة ما

الفيروس يبدأ العمل والتخريب وقد لا يكون هدف الفيروس التخريب هنا قد يكون هدفه ربحي كما حصل في إحدى المدن الانكليزية حيث تم توزيع قرص مجاني على المشافي به برنامج حول مرض الايدز (أسبابه – طرق انتشاره- طرق العلاج... الخ) وبعد مدة شهر من تشغيل البرنامج تم تشفير المعلومات على الحواسب الحاضنة للفيروس وظهرت رسالة مفادها إن الحاسب مصاب بالايدز (المقصود هنا انه تم تشفير ملفات الحاسب وإيقافها عن العمل بطريقة نظامية) أرسل مبلغ كذا إلى الحساب كذا ليتم إرسال رقم فك الشفرة مما اجبر المختصين بالرضوخ للطلب كونهم لم يستطيعوا فك التشفير . توجد عدة تقسيمات للفيروس ، فمثلا من حيث سرعة الانتشار هناك فيروسات سريعة الانتشار وفيروسات بطيئة الانتشار ومن حيث توقيت النشاط فيروسات تنشط في أوقات محددة وفيروسات دائمة النشاط ومن حيث مكان الإصابة فيروسات مقطع التشغيل bootsector على الأقراص وهي الأكثر شيوعا ، وفيروسات الماكرو macro التي تختص بإصابة الوثائق والبيانات الناتجة عن حزمة مايكروسوفت أوفيس ، أما من حيث حجم الضرر فهناك الفيروسات المدمرة للأجهزة طبعا لا يوجد فيروسات خارقة بحيث إنها تدمر الأجهزة كما نسمع أحيانا (احترق المعالج بسبب الفيروس تعطلت وحدة التغذية بسبب الفيروس أو تلفت الشاشة بسبب

الفيروس ،... الخ) ولكن يمكن للفيروس أن يؤذي الذاكرة روم في الحاسب كما في فيروس تشرنوبل أو أن يمحي معلومات MBR على القرص الصلب فتعود الأقراص الصلبة كما أتت من المصنع وفي الحالتين السابقتين لا يتم إقلاع الجهاز مما يوحي للبعض إن الفيروس (حرق) الحاسب طبعا تعتبر هذه الفيروسات خطيرة جدا لأنها تتسبب في إتلاف البيانات المخزنة والتي قد تكون (البيانات) نتاج عشرات السنين مما يؤدي إلى خسائر جسيمة أو إلى توقف الحاسبات عن العمل كما في تشرنوبل مما يؤدي إلى توقف الخدمات المقدمة، وهناك أيضا والفيروسات المدمرة للبرامج وتأثيرها محدود طالما إن البيانات لم تتأثر حيث يمكن تخزين البيانات وإعادة تهيئة الحاسب وإعادة البرامج

المتضررة من أقراصها الأصلية ، والفيروسات عديمة الضرر وهي التي لا تقوم بأي عمل مؤذي وإنما تم برمجتها لإثبات الذات والقدرة على البرمجة من بعض المراهقين فمنها ما يرسم كره على الشاشة طوال فترة عمل الكومبيوتر ومنها ما يغير بعض الأحرف (كتغير حرف بحرف أينما وجد) أو تغير مؤشر الماوس ...الخ .

24-Brontok

فيروس يخفي خيارات المجلد. هذا الفيروس من ابرز مهامه انه يقوم بإخفاء خيارات المجلد من قائمة أدوات الموجودة في نظام الويندوز وأيضا يقوم بتكرار جميع المجلدات التي يصيبها حتى انك لا تعرف الأصل من النسخة وقد تحذف الأصل ظنا منك انه الفيروس ، وهو أيضا يقوم بفتح شاشة الانترنيت اكسبلور ويقوم بفتح شاشة خضراء اللون بشكل مستمر مما يسبب بطء في النظام ومما يؤدي إلى زيادة انتشار هذا الفيروس في الكومبيوتر.

25-xcopy

والذي يصيب ال Partion القسم للقرص الصلب ويجعله لا يفتح مباشرة وذلك بزرع ملف auotorun وحينما تحاول فتح القسم يعطيك قائمة فتح باستخدام ولا تستطيع الدخول إلى القسم الذي تريده إلا بطرق ملتوية مثل (استكشاف وتشغيل) للمحترفين فقط ويقوم أيضا بجعل الفلوبي دسك القرص المرن يصيح باستمرار بإدخال قرص مرن للكومبيوتر .

الخلاصة

من خلال ما تم عرضه في متن البحث يمكن أن نعتبر النقاط التالية أهم ما تم التوصل إليه في البحث :-

١. تقسيم الفيروسات الهجومية فئتان الأولى هجومية (الحميدة) والفئة الثانية الهجومية (الخطرة أو المدمرة) .
٢. هناك أنظمة حماية من الفيروسات ونقصد بها المتداولة في الأسواق المحلية تعتبر غير جيدة نوعا ما وذلك لأنها مختصة بالفيروسات القديمة التي سبق وان دمرت أنظمة وأجهزة الكومبيوتر ولا يمكن لهذه الأنظمة الدفاعية أن تعرف إن كان هناك صدور لفيروس جديد إلا بعدما يظهر ذلك الفيروس ويقوم بتدمير أجهزة الكومبيوتر .
٣. نظام درع الفيروسات هو نظام مختص بمعالجة الفيروسات الخطرة أو المدمرة ويعتبر درع واقي من الفيروسات المعروفة القديمة والغير معروفة .
٤. ومن امتياز نظام درع الفيروسات انه لا يحتاج لعملية التحديث من المستخدم بمتابعة مستمرة لعملية ال update .
٥. تعتبر الثغرة من اخطر الوسائل التي يتم من خلالها انتقال الفيروسات ١الهجومية إلى الحاسوب .

٦. عندما يصيب الحاسوب بالفيروس الهجومي المدمر ويصده نظام درع الفيروسات ويقوم النظام بمعالجته وعليه سوف يشعر المستخدم بوجود أمر غير طبيعي لمدة ثانية أو ثواني أو ربما تعيق الجهاز ويعمل ثاني .

٧. الفيروسات الدفاعية هي عبارة عن حزمة من أوامر نظام التشغيل DOS يمكنه من استخدام أكثر من أمر في وقت واحد مما يسهل للمستخدم أمر CD و copy و format . وتوجد هناك عدد من الطرق التي يتم من خلالها عمل مثل هكذا ملفات والتي يمكن استعمالها كفيروسات دفاعية في الحاسوب .
٨. تعتبر طريقة تشفير الفيروسات من أفضل طرق الحماية لما لها من إمكانية لدمج الفيروس وتغير امتداد الفيروس أما سبب من bat إلى exe يمكنك تغيير امتداد ال Batch عن طريق برنامج Microsoft Visual Basic في الإصدار الخامس والسادس .
٩. الفيروسات المتجولة Polymorphic virus وهي الأصعب على برنامج المقاومة حيث انه صعب الإمساك بها وتتغير من جهاز إلى آخر في أوامرها .

Issam_art4@yahoo.com

2010